Hitachi Incident Response Team
2009.10.06 09:15:32 +09'00'

2008 年 HIRT 活動報告
HIRT: Annual Report 2008

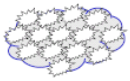
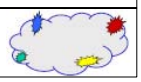
Hitachi Incident Response Team (HIRT)
http://www.hitachi.co.jp/hirt/

〒212-8567 神奈川県川崎市幸区鹿島田 890
Kashimada 890, Saiwai, Kawasaki, Kanagawa, 212-8567 Japan

1 はじめに

表 1は，2000 年以降のインシデントの変遷をまとめた表である．あくまでも主観的な視点からまとめた表であるため，必ずしもすべてのインシデントを網羅しているものではない．しかし，数年間のインシデントの変遷を見る限り，短いサイクルで新たな侵害活動が生まれ，一度確立した侵害活動は決してなくなることはなく，さらに侵害活動を通して良くも悪くも技術が継承されている．また，2008 年から流布しはじめた USB メモリを介したウイルス(以降，USB メモリ型ウイルス)感染は，フロッピーディスクを介した流布の再来，まさに歴史は繰り返していると言えよう．

表 1：2000 年以降のインシデントの変遷

年代	特徴	被害の模式図
2000年 ～2001年	均一的かつ広範囲に渡る単発被害 Webサイトのページ書き換え	
2000年 ～2005年	均一的かつ広範囲に渡る連鎖型被害 ウイルス添付型メールの流布 ネットワーク型ワームの流布	
2005年～	類似した局所的な被害 SQLインジェクションによるWebサイト侵害 Winny、Shareによる情報流出 フィッシング、スパイウェア、ボットなど	
2006年～	すべてが異なる局所的な被害 標的型攻撃	

このようなインシデントの変化は，対処側の考え方にも反映され，1988 年のインターネットワームの出現を契機に，インシデントの原因や対応方法に関する情報共有の重要性が認識され，あらかじめ決めておいた計画に沿って事後対処する『インシデントレスポンス』という考え方が普及し始めた．また，2001 年から 2003 年にかけ流布したネットワークワームの対処を通じて，インシデントに伴う被害を予測ならびに予防し，インシデント発生後は被害の拡大を低減するために実施する一連のセキュリティ対策活動である『インシデントオペレーション』という考え方が生まれた．

さらに，変化は，CSIRT(Computer Security Incident Response Team)に，情報セキュリティ対策活動として脆弱性対策やインシデント対応を推進するための『技術的な視点で脅威を推し量り，伝達できること』『技術的な調整活動ができること』『技術面での対外的な協力ができること』という基本的な能力に加えて，経験値を活かした次のような役割も求めている．

『次の脅威をキャッチアップする』
過程の中で，早期に対策展開を図る．

HIRT(Hitachi Incident Response Team)は，これら能力ならびに役割を持った組織として，製品ならびにサービスの脆弱性対策，ウイルス被害や情報漏えいなどのインシデント対応を先導すると共に，セキュリティ分野での日立ブランドを向上するための活動，仕組みならびに体制を整備する日立グループの IRT 統一窓口組織としての責務を負っている．

本稿では，2008 年の HIRT 活動の報告として，2008 年の脅威と脆弱性の概況と HIRT の活動トピックスについて報告する．

2 2008 年の活動概要

本章では，2008 年の HIRT の活動トピックスを中心に報告する．

2.1 脅威と脆弱性の概況

2008 年は，DNS キャッシュポイズニング，USB メモリ型ウイルス, MS08-067 を悪用するネットワーク型ワーム，SQL インジェクション攻撃など，以前から知られている侵害手法，あるいは，過去に流行した侵害手法の再発などが見られた．また，Web サイトは，侵入したマルウェアが他の機能を持つプログラム群を繰り返しダウンロードするための機能変更ダウンロードサイトとしても活用されている状況にある．

脆弱性については図 1に示す通り，NIST NVD(National Vulnerability Database)に登録された 2008 年の脆弱性の総件数は 5,634 件(CERT/CC の

報告は 6,058 件)で減少傾向にある．しかし，その中で Web アプリケーション系ソフトウェア製品の脆弱性(クロスサイトスクリプティング(XSS), SQL インジェクション，ディレクトリ・トラバーサル，クロスサイト・リクエスト・フォージェリ(CSRF))が約 40%, 2,315 件となっている(図 2)[1]. また，IPA に報告された稼動中 Web サイトの脆弱性のうち，約 6 割がクロスサイトスクリプティング(XSS)，SQL インジェクションによって占められており，これら脆弱性の報告件数も年々増加傾向にある(図 3)[2].

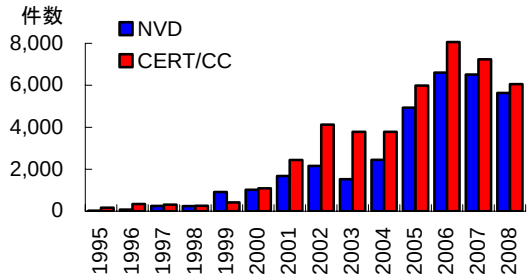


図 1：脆弱性報告件数の推移(出典：NIST NVD)

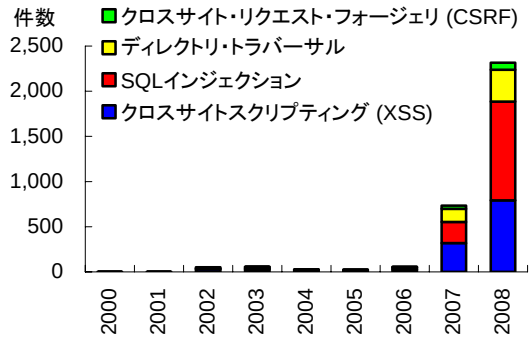


図 2：Web アプリケーション系ソフトウェア製品の脆弱性報告件数の推移(出典：NIST NVD)

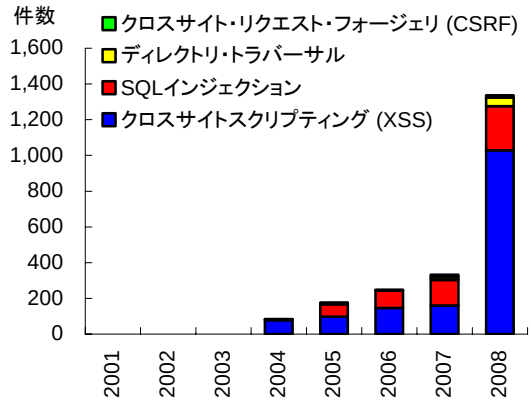


図 3：Web サイトの脆弱性報告件数の推移
(出典：IPA，JPCERT/CC)

さらに，2007 年以降 SQL インジェクションに関する攻撃検知数が増加していることから(図 4)[3]，Web サイトが侵害活動の基点にならないよう，脆弱性対策の一層の推進が必要となっている．

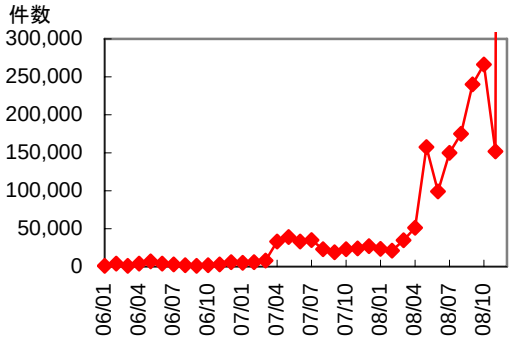


図 4：SQL インジェクション攻撃検知数の推移
(出典：LAC)

DNS キャッシュポイズニングは，DNS サービスを提供しているサーバ(DNS サーバ)に偽の情報を覚えこませる攻撃手法である．攻撃が成功すると，DNS サーバは覚えた偽の情報を提供してしまう．このため，ユーザは正しいホスト名の Web サーバに接続しているつもりでも，提供された偽の情報により，攻撃者が罠をはった Web サーバに誘導されてしまうことになる．これまでも，DNS キャッシュポイズニングの潜在的な脅威について指摘されてきた．しかし，2008 年 7 月に，効率的にキャッシュポイズニング可能な手法が公開されたことから，インターネット基盤サービスでもある DNS サービスを保護するため広く対策を浸透させていく必要がある(図 5).

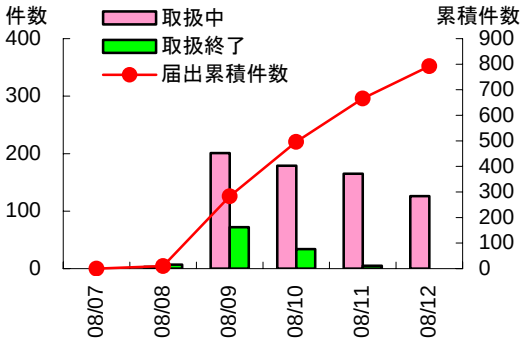


図 5：DNS キャッシュポイズニング届出件数と対策状況(出典：IPA，JPCERT/CC)

2008 年から流布しはじめた USB メモリ型ウイルスについては，感染被害の報告件数が確実に増えてきており(図 6)[4]，物理的な媒介手段として定着しつつある．USB メモリの自動再生／自動実行という利便性と安全性については，予防措置として見直しが必要となっていると言える．

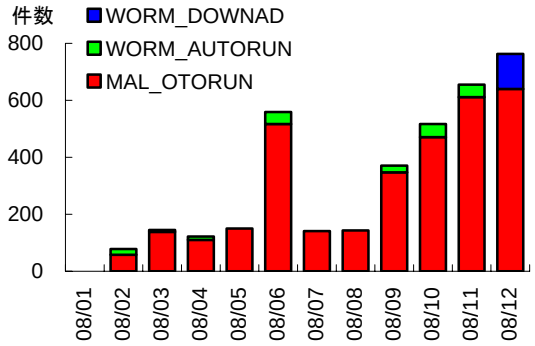


図 6：USB メモリ型ウイルスの感染被害報告数
(出典：トレンドマイクロ)

2.2 HIRT の活動トピックス

本節では，2008 年の活動トピックについて述べる．

(1) 演習型 HIRT オープンミーティングの定着化

HIRT オープンミーティングは，信頼関係に基づく HIRT コミュニティを普及させるための活動である．『HIRT 活動に関して，HIRT センタに所属するメンバ同士が情報交換する場である』『HIRT センタの活動内容について，日立グループに広く知ってもらうことと，HIRT センタ以外からの意見を広く取り入れるために，情報交換する場を公開する』『公開の場を通じて，信頼関係に基づく HIRT コミュニティへの参加を募る』という方針に沿って開催している．

2008 年は，2007 年から開始した Web アプリケーション開発を対象とした演習型 HIRT オープンミーティング(図 7)の定着化を目指し，計 9 回(受講者：約 200 名)のミーティングを開催した．

【 タイムテーブル 】
(1) Webアプリケーションセキュリティの動向 (10分)
(2) 日立グループでの取組み状況／演習の目的 (20分)
(3) Webアプリケーションの脆弱性の解説 (60分)
(4) 脆弱性検査演習 (各自演習) (70分)
(5) 脆弱性報告書の作成 (各自演習) (30分)
(6) Webアプリケーションセキュリティガイド (30分)
及び機能要件チェックリストの紹介
(7) SQLインジェクションログチェックツール紹介 (10分)

図 7：演習型 HIRT オープンミーティング
(Web アプリケーションのセキュリティ)

(2) 製品／サービスセキュリティ活動の整備

脆弱性対策ならびに，インシデント対応などの活動を通じて得られたノウハウを製品開発プロセスにフィードバックするため，各プロセスにあった HIRT 支援活動の体系化の検討を開始した．支援活動が先行している Web アプリケーションのセキュリティについては，項番(1)の演習型 HIRT オープンミーティングを取り込んだ体系化を検討している(図 8).

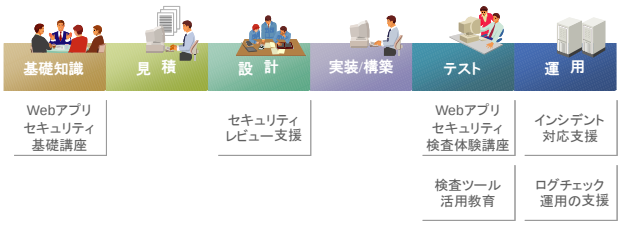


図 8：HIRT 支援活動の体系化
(Web アプリケーションのセキュリティ)

組込み系製品については，セキュリティを考慮した製品開発プロセスを整備していくために，セキュリティ評価に対する考え方や進め方，ツール活用方法などセキュリティ検査を対象とした支援活動を開始した．特に，セキュリティ検査に利用するツールについては，SIP(Session Initiation Protocol)など製品個別のセキュリティ検査ツールの開発／提供だけではなく，IPA から TCP/IP を実装する製品開発者向けに提供されている『TCP/IP に係る既知の脆弱性検証ツール』[5]を活用することで，既に公表されている脆弱性の再発を防ぐと共に，日立グループ内における情報家電／組込み系製品／制御系製品におけるセキュリティ施策の具体化を進めている．

また，製品／サービスセキュリティ活動を浸透させていくためには，技術面だけではなく，常に『今どのような状況なのか』『何が問題なのか』『どのような対処策があるのか』を検討し，行動に移せるマインドフルな組織[6]であることが重要である．そこで，2008 年 4 月，明治大学 経営学部 教授 中西晶氏を講師として招き，障害や事故といった不測の事態に強い組織，高信頼性組織(High Reliability Organization)についての講演会を開催した．

(3) DNS キャッシュポイズニングの対策支援

DNS サービスに伴う DNS キャッシュポイズニングの脅威を低減するために，2008 年 8 月に注意喚起を行った．さらに，インターネット上の多くネットワークサービスが DNS を前提としているにも関わらず，DNS の動作や関連ツールの情報はあまり普及していない状況を踏まえ，12 月に DNS キャッシュポイズニング対策の一環として，DNS の動作やツールの使い方に踏み込んだ『DNS の役割と関連ツールの使い方』説明会を開催した(図 9). また，説明会用に作成した資料は，国内の DNS キャッシュポイズニング対策の推進に役立ててもらうため，2009 年 1 月に IPA から発行された『DNS キャッシュポイズニング対策』[7]の資料素材とし

て提供した.

【タイムテーブル】
(1) HIRT-08043 の解説 (10分)
(2) DNSの動作と関連ツール (20分)
- whois サービス
- nslookup コマンド
(3) 検査ツールの使い方と注意点 (30分)
- Cross-Pollination Check
- DNS-OARC Randomness Test
(4) 再帰問合せ設定 (20分)
- BIND DNSサーバでの対策
- Windows DNSサーバでの対策
(5) HIRT-FUP活動紹介とご協力のお願い (5分)

図 9：DNS キャッシュポイズニング対策説明会

(4) JWS2008 の開催

2008 年 3 月，国内 FIRST 加盟チームと共に，FIRST 技術ミーティングである FIRST Technical Colloquium(2008 年 3 月 25 日～28 日)を東京に誘致した．また，期間中，国内 CSIRT 間の強い信頼関係に基づいた迅速かつ最適な体制作りを推進するための意見交換の場となることを目指したワークショップ Joint Workshop on Security 2008, Tokyo(JWS2008)を開催した[8].

(5) 国内 COMCHECK Drill 2008 への参加

国内 COMCHECK Drill 2008(演習名：SHIWASU, 2008 年 12 月 4 日実施)は，日本シーサート協議会が主催した国内の CSIRT，企業内の情報セキュリティ部署の対外向け連絡窓口のコミュニケーション確認を目的とした訓練である．演習は，全体を指揮する取りまとめ者と各組織の連絡窓口をスター型に構成し，インシデント発生を想定したメール連絡を実施した.

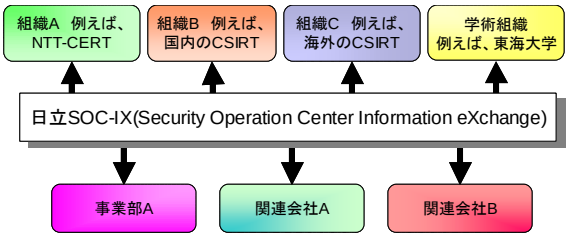
(6) CSIRT コミュニティとの組織間連携の強化

組織間連携強化の具体的な活動として，NTT-CERT[9]と定期的な会合を開催し，CSIRT 活動自身を改善するための情報交換ならびに，マルウェア捕獲システム(Nepenthes)の相互利用を実施した．マルウェア捕獲システムについては，収集したデータを元に，感染動作に着目した調査結果を情報処理学会コンピュータセキュリティ研究会にて発表することで，組織間連携の取り組みを形にしていく試みも実施した[10].

また，継続的に発生しているファイル交換ソフトウェアを介した情報漏えいについては，社外との組織間連携が必要であると考え，2007 年に引き続き，システム開発研究所と共に，総務省委託研究『ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発』に参画するコンピュータソフトウェア著作権協会，安心・安全インターネット推進協議会 P2P 研究会の協力を得て，ファイル交換ネットワーク環境の調査活動を実施した[11][12].

新たな組織間連携の取り組みとして，標的型攻撃の実態の一旦を明らかにすべく，情報処理学会コンピュータセキュリティ研究会が主催するシンポジウムの CFP(Call For Papers)を騙ったウイルス添付メールの検体を関連組織に提供すると共に，ウイルス添付メール受信を安全に体験可能な仮想体験デモ[*]を提供した[13].

徐々にではあるが，『脅威分析』に必要となる観測データなどの情報を組織間で相互活用していくためのフレームワークである『日立 SOC-IX(Security Operation Center Information eXchange)』が立ち上がり始めた 1 年であった(図 10).



観測データなどの情報を交換する場所と仕組みを作ることによる利点
・多種多様で、多量の観測データを使った分析
・自組織では持っていない観測データの活用
・各CSIRTが得意とする分野の技術やノウハウの活用

図 10：日立 SOC-IX の概念図

(7) その他

- システム開発研究所と協力し，総務省委託研究『ネットワークを通じた情報流出の検知及び漏出情報の自動流通停止のための技術開発』の研究成果をレポート形式にまとめて HIRT の Publications コーナーに掲載(表 2).
- 日経 BP 社 ITpro CSIRT(Computer Security Incident Response Team)フォーラムに，脆弱性対策に関する記事を寄稿

表 2：Publications コーナー掲載レポート

番号	題名
HIRT-PUB08008	2008 年ファイル交換ソフトによる情報漏えいに関する調査結果
HIRT-PUB08007	P2P ファイル交換ソフト環境で流通するマルウェア
HIRT-PUB08005	DNS サーバにおけるキャッシュポイズニング対策
HIRT-PUB08002	みんなで「情報セキュリティ」強化宣言！2008
HIRT-PUB08001	クローリング調査を用いたファイル交換ソフトのノード数推定

*) 仮想体験デモは、ボタン操作(デモ開始、少しだけ巻き戻し)の可能な Flash ファイルのムービーであり、デモ開始により実際のウイルス感染活動が発生するわけではない。

3 HIRT

本章では, HIRT に対する理解を深めてもらうために，組織編成モデル，調整機関である HIRT センタの位置付け，ならびに現在 HIRT センタが推進している活動について述べる．

3.1 組織編成モデル

HIRT では, 4 つの IRT という組織編成モデルを採用している(図 11，表 3)．4 つの IRT とは，日立グループが，情報システム関連製品を開発する側面(製品ベンダ IRT), その製品を用いたシステムを構築やサービスを提供する側面(SI ベンダ IRT), そして，インターネットユーザとして自身の企業情報システムを運用管理していく側面(社内ユーザ IRT)の 3 つがあること，これらの IRT 間の調整業務を行なう HIRT/CC(HIRT Coordination Center)を設けることにより，各 IRT の役割を明確にしつつ，IRT 間の連携を図った効率的かつ効果的なセキュリティ対策活動を推進できると考えたモデルである．なお，HIRT という名称は，広義の意味では日立グループ全体のインシデントオペレーション活動を示し，狭義の意味では，HIRT/CC(HIRT センタ)を示している．

実際に，4 つの IRT が整備されるまでには表 4にある 4 段階ほどのステップを踏んでおり，3 つの IRT の大枠が決まった後に，社内外の調整役となる HIRT センタが組織として構成されている．また，各段階においては組織編成を後押しするトリガが存在している．例えば，第 2 ステップの製品ベンダ IRT 立上げには CERT/CC から報告された SNMP の脆弱性[14]が多くの製品に影響を与えたこと, 第 3 ステップの SI ベンダ IRT 立上げについては『情報セキュリティ早期警戒パートナーシップ』の運用開始が挙げられる．

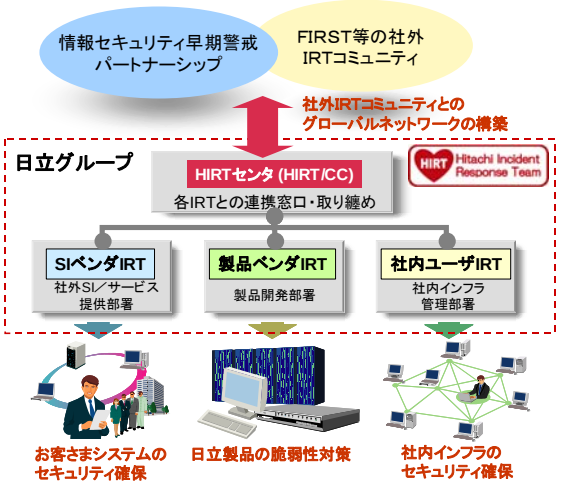


図 11：組織編成モデルとしての 4 つの IRT

表 3：各 IRT の役割

分類	役割
HIRT/CC	該当部署：HIRT センタ ➢ FIRST，JPCERT/CC，CERT/CC などの社外 CSIRT 組織との連絡窓口 ➢ SI ベンダ／製品ベンダ／社内ユーザ IRT 組織間の連携調整
SI ベンダ IRT	該当部署：SI／サービス提供部署 ➢ 顧客システムを対象とした CSIRT 活動の推進 ➢ 公開された脆弱性について，社内システムと同様に顧客システムのセキュリティを確保
製品ベンダ IRT	該当部署：製品開発部署 ➢ 日立製品の脆弱性対策，対策情報公開の推進を支援 ➢ 公開された脆弱性について影響有無の調査を迅速に行い，該当する問題については，告知修正プログラムの提供
社内ユーザ IRT	該当部署：社内インフラ提供部署 ➢ 日立サイトが侵害活動の基点とならないよう社内ネットワークのセキュリティ対策の推進を支援

表 4：組織編成の経緯

ステップ	概要
1998 年 4 月	日立としての CSIRT 体制を整備するためのプロジェクトとして活動を開始
第 1 ステップ 社内ユーザ IRT の立上げ (1998 年～2002 年)	日立版 CSIRT を試行するために，日立グループに横断的なバーチャルチームを編成し，メーリングリストをベースに活動を開始. メンバ構成は主に社内セキュリティ有識者及び社内インフラ提供部門を中心に編成.
第 2 ステップ 製品ベンダ IRT の立上げ (2002 年～)	製品開発部門を中心に, 社内セキュリティ有識者，社内インフラ提供部門，製品開発部門，品質保証部門等と共に，日立版 CSIRT としての本格活動に向け, 関連事業所との体制整備を開始.
第 3 ステップ SI ベンダ IRT の立上げ (2004 年～)	SI／サービス提供部門と共に SI ベンダ IRT の立上げを開始. さらに，インターネットコミュニティとの連携による迅速な脆弱性対策ならびにインシデント対応の実現に向け，HIRT の対外窓口ならびに社内の各 IRT との調整業務を担う HIRT/CC の整備を開始.
2004 年 10 月	HIRT/CC として HIRT センタを設立.

3.2 HIRT センタの位置付け

HIRT センタは，情報・通信グループ配下に設置された製品／サービスセキュリティ委員会の実行組織である．主な活動は，情報セキュリティ統括部，情報システム事業部と品質保証本部との相互協力による制度面／技術面でのセキュリティ対策活動の推進，各事業部／グループ会社への脆弱性対策ならびにインシデント対応の支援，そして，日立グループの CSIRT 窓口として組織間連携によるセキュリティ対策活動の促進である(図 12).

また，HIRT センタの組織編成上の特徴は，縦軸の組織と横軸のコミュニティが連携するモデルを採用しているところにある．具体的には，専属者

と兼務者から構成されたバーチャルな組織体制をとることで，フラットかつ横断的な対応体制と機能分散による調整機能役を実現している．このような組織編成の背景には，情報システムの構成品が多岐にわたっているため，セキュリティ問題解決のためには，各部署の責務推進と部署間の協力が必要であるとの考えに基づいている．

3.3　HIRT センタの主な活動内容

現在推進している HIRT センタの主な活動は，社内向けの CSIRT 活動(表 5)と，社外向けの CSIRT 活動(表 6)とがある．

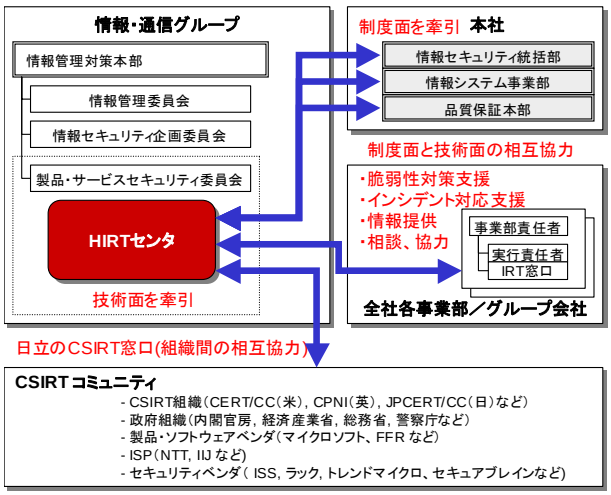


図 12：HIRT センタの位置付け

表 5　推進中のプロジェクト(社内対応)

分類	概要
セキュリティ情報の収集／分析／提供	➢ 情報セキュリティ早期警戒対応の推進(脆弱性対策ならびにインシデント対応に関する情報／ノウハウの水平展開) ➢ 日立 SOCIX(Security Operation Center Information eXchange)に基づく広域観測網の構築 ➢ マルウェア対策のための技術ノウハウの蓄積と展開
製品／サービスの脆弱性対策とインシデント対応の推進	➢ セキュリティ情報統合サイトを活用した社外 Web サイトにおけるセキュリティ情報発信基盤の整備 ➢ 社内セキュリティ情報発信基盤の整備
製品／サービスのセキュリティ技術の向上	➢ Web アプリケーションセキュリティの強化 ➢ 情報家電／組込み系製品／制御系製品におけるセキュリティ施策の具体化 ➢ 脆弱性対策のための技術ノウハウの蓄積と展開 ➢ 開発／管理プロセスの整備(開発～検査～運用管理のための各種ガイドラインなど)
研究活動基盤の整備	➢ システム開発研究所との共同研究体制の整備(P2P 観測関連など)

社内向けの CSIRT 活動では，セキュリティ情報の収集／分析を通して得られたノウハウを注意喚起やアドバイザリとして発行し，また，各種ガイドラインや支援ツールの形で製品開発プロセスにフィードバックする活動を推進中である．

社内向けの注意喚起やアドバイザリの発行については，2005 年 6 月から HIRT セキュリティ情報の細分化として，注意喚起ならびに注目すべき情報を広く配布することを目的とした HIRT セキュリティ情報と，個別に対処依頼を通知する HIRT-FUP 情報とに分け，広報と優先度とを考慮した運用に移行している(表 7，図 13)．また，情報を効果的に展開するため，情報の集約化による発行数の低減と共に，情報セキュリティ本部と品質保証本部と連動した情報発信を実施している．

また，製品／サービスの脆弱性対策とインシデント対応として，セキュリティ情報統合サイトを用いて，日立グループの製品／サービスセキュリティに関する取り組みを広くインターネットユーザに展開する活動を推進中である．

表 6　推進中のプロジェクト(社外対応)

分類	概要
CSIRT 活動の国内連携の強化	➢ 情報セキュリティ早期警戒パートナーシップに基づく脆弱性対策活動の展開 ➢ 日本シーサート協議会関連活動の推進
CSIRT 活動の海外連携の強化	➢ FIRST カンファレンスならびにシンポジウムでの講演／参画を通じた海外 CSIRT 組織／海外製品ベンダ IRT との連携体制の整備 ➢ 英国 WARP 関連活動の推進 ➢ CVE，CVSS，CPE など脆弱性関連の標準化への対応
研究活動基盤の整備	➢ 東海大学(菊池教授)との共同研究の推進 ➢ マルウェア対策研究人材育成ワークショップなど学術系研究活動への参画

表 7：HIRT が発行するセキュリティ情報の分類

識別番号	用途
HIRT-FUPyynnn	優先度：緊急 配布先：関連部署のみ HIRT メンバが日立グループ製品や Web サイトの脆弱性を発見した場合，またはその報告を受けた場合など，関連部署との連絡を必要とする際に利用する．
HIRT-yynnn	優先度：中～高 配布先：限定なし 広く脆弱性対策ならびにインシデント対応の注意喚起を行なう際に利用する．
HIRT-FYIyynnn	優先度：低 配布先：限定なし HIRT オープンミーティング，講演会などの開催案内を通知する際に利用する．

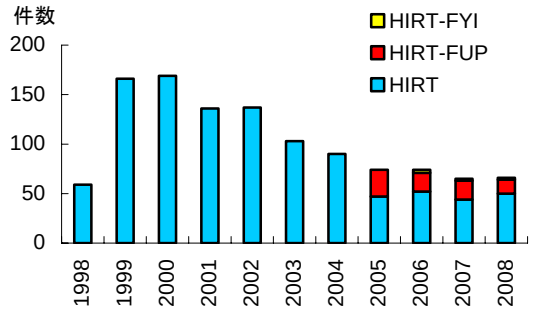


図 13：識別番号別セキュリティ情報の発行数

特に，社外向けの脆弱性対策ならびにインシデント対応のセキュリティ情報の発信にあたっては，セキュリティ情報統合サイトを用いた定常的なセキュリティ情報の発信だけではなく，『緊急度のレベル』を判断し，次に情報掲載 Web サイトの『階層レベル』を選択するという緊急度レベル×階層レベル型の情報発信アプローチも併用している(図 14).

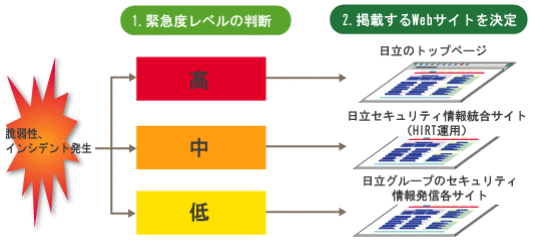


図 14:緊急度レベル×階層レベル型の情報発信の概念図

4　1998 年～2007 年の活動サマリ

本章では，HIRT プロジェクトとして活動を始めた 1998 年以降の各年の活動トピックスについて述べる.

4.1　2007 年

(1) 演習型 HIRT オープンミーティングの開始

2007 年は，3 月，6 月の 2 回，Web アプリケーション開発者を対象に，演習型の HIRT オープンミーティングを開催し，ガイドライン『Web アプリケーションセキュリティガイド』のより実践的な展開を実施した.

(2) 日本シーサート協議会の設立

2007 年 4 月，単独の CSIRT では解決が困難な事態に対して CSIRT 間の強い信頼関係に基づいた迅速かつ最適な対応を実施する体制作りを整備するため，IIJ-SECT(IIJ)，JPCERT/CC，JSOC(ラック)，NTT-CERT(NTT)，SBCSIRT(ソフトバンク)と共に，日本シーサート協議会を設立した[15].

(3) 英 WARP 加盟

2007 年 5 月，CSIRT 活動の海外連携強化のため，英国政府のセキュリティ機関 CPNI(The Centre for the Protection of the National Infrastructure)が推進する WARP(Warning, Advice and Reporting Point)に加盟した[16].

(4) CSIRT コミュニティとの組織間連携の強化

組織間連携強化の具体的な活動として，2006 年から NTT-CERT[9]と定期的に会合を開催し，CSIRT 活動自身を改善するための情報交換を続けている．2007 年は，NTT-CERT とのボット観測の相互協力関係を整備するため，観測データの相互利用の検討を実施した.

(5) 講演会

- 2007 年 8 月：フォティーンフォティ技術研究所 鵜飼裕司氏『静的解析による脆弱性検査』

4.2　2006 年

(1) 脆弱性届出統合窓口の設置

2006 年 11 月，日立グループにおいて脆弱性関連情報を適切に流通させ，日立のソフトウェア製品および Web サイトの脆弱性対策を推進するために，ソフトウェア製品および Web アプリケーションに関する脆弱性もしくは不具合を発見した場合の日立グループ向け脆弱性届出統合窓口を設置した.

(2) Web アプリケーションセキュリティの強化

2006 年 10 月，日立グループにおける Web アプリケーションセキュリティ施策の一環として，ガイドラインとチェックリストを整備すると共に，日立グループ内への展開を支援した．ガイドライン『Web アプリケーションセキュリティガイド(開発編)V2.0』では，LDAP インジェクション，XML インジェクションなどの新たな脆弱性項目と脆弱性有無の確認方法を追記し改訂を行った.

(3) ファイル交換ソフトによる情報漏えいに関する注意喚起

Antinny は，2003 年 8 月に出現したファイル交換ソフトウェア『Winny』を通じて流布するウイルスであり，感染に伴う情報漏えいや特定サイトへの攻撃を伴う．HIRT では，これら脅威の状況を踏まえ，2006 年 4 月に資料『～ウィニーによる情報漏えいの防止と将来発生する危険から身を守るために～』による注意喚起を行った.

(4) 情報家電／組込み系の製品セキュリティ活動の立上げ

情報家電／組込み系の製品セキュリティ活動の立上げを開始した．HIRT では，インターネット電話などで用いられる通話制御プロトコルのひとつである SIP(Session Initiation Protocol)に注目し，関

連するセキュリティツールならびにセキュリティ対策の状況を調査報告としてまとめた.

(5) CSIRT コミュニティとの組織間連携の強化

2006 年 3 月，NTT-CERT 主催の NTT グループ向けワークショップで日立の CSIRT 活動を紹介し，CSIRT 活動自身を相互に改善するための情報交換を行なった.

(6) 講演会

- 2006 年 5 月 : eEye Digital Security 鵜飼裕司氏『組込みシステムのセキュリティ』
- 2006 年 9 月 : Telecom-ISAC Japan 小山覚氏『Telecom-ISAC Japan におけるボットネット対策』

(7) その他

- HIRT から発信する技術文書(PDF ファイル)にデジタル署名を付加する活動の開始[17]

4.3 2005 年

(1) FIRST 加盟

2005 年 1 月, 各国の CSIRT 組織と連携可能なインシデント対応体制を作りながら，CSIRT 活動の実績を積むため，世界におけるコンピュータインシデント対応チームの国際的なコミュニティである Forum of Incident Response and Security Teams(FIRST)に加盟した[18]. 加盟にあたっては，加盟済み 2 チームによる推薦が必要であり，約 1 年の準備期間を要した.

2009 年 1 月現在，日本からは，CFC(警察庁情報通信局)，HIRT(日立)，IIJ-SECT(IIJ)，IPA-CERT(情報処理推進機構)，JPCERT/CC，JSOC(ラック)，KKCSIRT(カカクコム)，NCSIRT(NRI セキュアテクノロジーズ)，NISC(内閣官房情報セキュリティセンタ)，NTT-CERT(NTT)，Rakuten-CERT(楽天)，RicohPSIRT(リコー)，SBCSIRT(ソフトバンク)，YIRD(ヤフー)の 14 チームが加盟している(図 15).

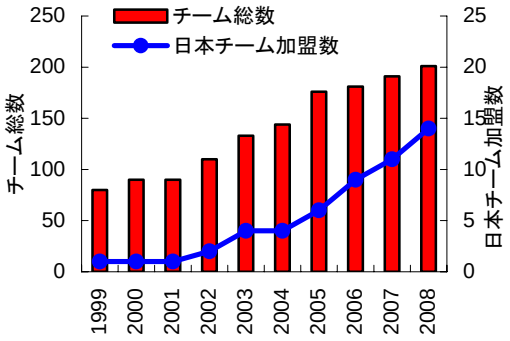


図 15：FIRST 加盟チーム数の推移

(2) セキュリティ情報用の統合窓口ページ (セキュリティ情報統合サイト)の開設

2005 年 9 月，日立グループの製品／サービスのセキュリティ問題に関する情報を統合的にインターネット利用者に提供するため，各事業部ならびにグループ会社の Web サイトから発信されているセキュリティ情報を統合する窓口ページを開設した(図 16). これにあわせ，セキュリティ情報発信ガイドとして『社外向け Web セキュリティ情報発信サイトの発信ガイド V1.0』を作成した.

セキュリティ情報統合サイト
日本語　http://www.hitachi.co.jp/hirt/
英語　http://www.hitachi.com/hirt/

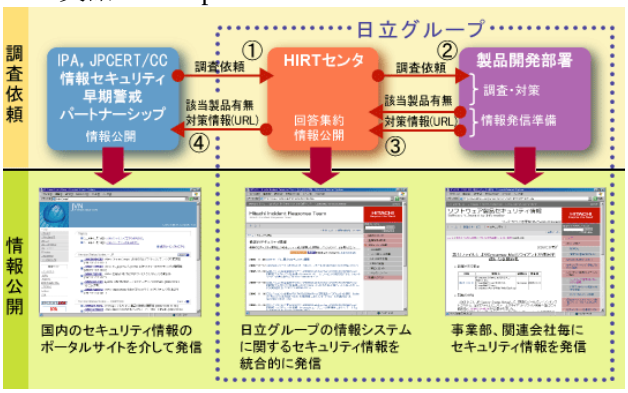


図 16：統合サイトでのセキュリティ情報発信

(3) CSIRT 活動の国内連携強化

CSIRT 活動の国内連携強化として，FIRST 加盟済み国内チームとのミーティング，NTT-CERT ならびにマイクロソフト PST(Product Security Team)との個別チームミーティングを実施すると共に，Web サイト改ざん発見時の通知などの連絡網を整備した.

4.4 2004 年

(1) 情報セキュリティ早期警戒パートナーシップへの参画

2004 年 7 月『ソフトウェア等脆弱性関連情報取扱基準』の施行にあわせて，情報セキュリティ早期警戒パートナーシップ制度が始動した[19][20], 日立グループでは，パートナーシップに製品開発ベンダ登録(HIRT を連絡窓口)すると共に，JP Vulnerability Notes(JVN)[21]に脆弱性対策の状況掲載を開始した.

(2) Web アプリケーションセキュリティの強化

2004 年 11 月，Web アプリケーションの設計／開発時に留意すべき，代表的な問題点とその対策方法の概要についてまとめた『Web アプリケーションセキュリティガイド(開発編)V1.0』を作成し，日立グループ全体に展開した.

(3) 講演会

- 2004 年 1 月 : ISS(Internet Security Systems)Tom Noonan 氏 『Blaster 以降の米国セキュリティビジネス事情』

4.5 2003 年

(1) Web アプリケーションセキュリティ活動の立上げ

Web アプリケーションセキュリティ強化スキームの検討を開始すると共に，事業部と共同で，『Web アプリケーション開発に伴うセキュリティ対策基準の作成手順 V1.0』を作成した.

(2) NISCC からの脆弱性関連情報の社内展開

2002 年の CERT/CC 脆弱性関連情報の社内展開に続き，NISCC(現 CPNI)Vulnerability Disclosure Policy に基づく脆弱性関連情報入手と情報掲載を開始した. 活動開始以降, 日立製品の情報が NISCC Vulnerability Advisory に最初に掲載されたのは 2004 年 1 月の 006489/H323 である[22].

(3) HIRT 社外向け連絡窓口の整備

脆弱性発見に伴う関連機関への報告と公開に関する活動[23][24][25]の活発化にあわせ，日立製品ならびに日立が関与するサイトに対して脆弱性の存在や侵害活動の要因などが指摘された場合の対処窓口として，表 8に示す連絡窓口を設置した.

表 8：連絡窓口情報

名称	"HIRT": Hitachi Incident Response Team.
所在地	〒212-8567 神奈川県川崎市幸区鹿島田 890
電子メールアドレス	hirt@hitachi.co.jp
公開鍵 PGP key	KeyID = 2301A5FA Key fingerprint 7BE3 ECBF 173E 3106 F55A 011D F6CD EB6B 2301 A5FA pub 1024D/ 2003-09-17 HIRT: Hitachi Incident Response Team < hirt@hitachi.co.jp >

4.6 2002 年

(1) CERT/CC 脆弱性関連情報の社内展開

2002 年に CERT/CC から報告された SNMP の脆弱性[14]は，多くのソフトウェアや装置に影響を与えた. この脆弱性報告をきっかけに, HIRT では, 製品ベンダ IRT の立上げ，CERT/CC Vulnerability Disclosure Policy に基づく脆弱性関連情報入手と情報掲載を開始した[26]. 活動開始以降，日立製品の情報が CERT/CC Vulnerability Notes Database に最初に掲載されたのは 2002 年 10 月の VU#459371 である[27].

(2) JPCERT/CC Vendor Status Notes の構築支援

国内のセキュリティ情報流通改善の試みとして, 2003 年 2 月, 試行サイト JPCERT/CC Vendor Status Notes(JVN)の(http://jvn.doi.ics.keio.ac.jp/)の構築と運用を支援した(図 17)[28][29]. なお，試行サイトは，2004 年 7 月の『ソフトウェア等脆弱性関連情報取扱基準』の施行に伴い，報告された脆弱性を公表する Japan Vulnerability Notes(JVN)サイト(http://jvn.jp/)にその役割を引き継いでいる.

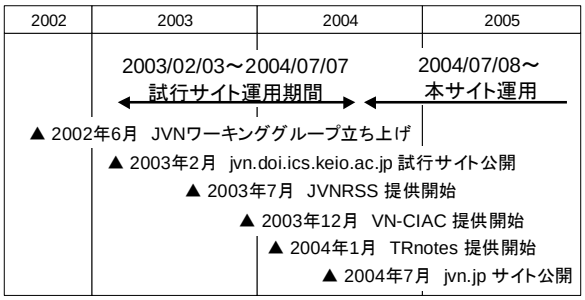


図 17：JVN 試行サイトの構築ならびに運用

4.7 2001 年

(1) Web サービスを攻撃対象とするワームの活動状況調査

インターネット上に公開している Web サイトから回収したログデータをもとに，2001 年に流布した Web サービスを攻撃対象とするワームである，CodeRed I，CodeRed II，Nimda の活動状況について状況調査を実施した(2001 年 7 月 15 日～2002 年 6 月 30 日). 特に，国内で被害の大きかった CodeRed II，Nimda(図 18)については，最初の痕跡記録時刻から最頻数となった日までわずか 2 日間程度であり，ワームによる被害波及が短期間かつ広範囲に渡っていた.

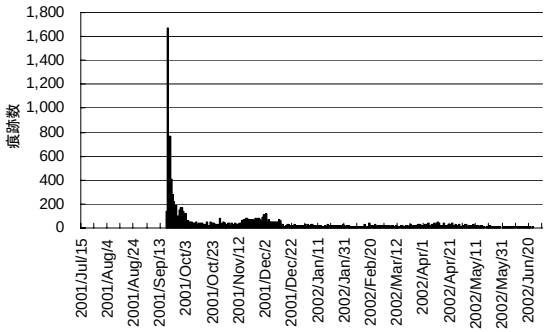


図 18：観測期間内の痕跡数変位(Nimda)

4.8　2000 年

(1) 脆弱性の深刻度に関する指標調査

侵害活動などに利用される脆弱性の深刻度を図るために，関連機関が提示している脆弱性の深刻度の指標を調査し，調査報告としてまとめた．

CERT/CC では，脆弱性毎に Vulnerability Notes[30]と呼ぶメモを作成し，その中で脆弱性の深刻度を示す Severity Metrics を算出している[31]. CVE(Common Vulnerabilities and Exposures)では脆弱性を『通常考えられる一般的なセキュリティポリシーを侵害する“Vulnerability”』と『個々の環境に依存し，個別のセキュリティポリシーを侵害する“Exposure”』の 2 つに区別し，Vulnerability を脆弱性として取り扱う[32]．また，NIST では，NVD の前身である ICAT Metabase[33]において，CERT アドバイザリならびに CVE の発行有無を脆弱性の深刻度判定の目安とし，3 段階の分類を行っている．

なお，各組織で使用する脆弱性の深刻度指標が異なっていることから，2004 年，脆弱性の深刻度を包括的かつ汎用的に評価する共通言語として CVSS(Common Vulnerability Scoring System)[34]が提案された．

4.9　1999 年

(1) hirt.hitachi.co.jp ドメイン稼動開始

日立グループへのセキュリティ情報提供の改善を図るため，1999 年 12 月，HIRT プロジェクト用の社内向けドメインを用意し，Web サイト hirt.hitachi.co.jp を立上げた．

(2) Web サイト書き換えの調査

1996 年に米国で Web サイトのページ書き換えが発生してからネットワークワーム世代(2001 年～2004 年)までの間，Web サイトのページ書き換えが代表的なインシデントとなったことから，1999 年～2002 年にかけ，侵害活動の発生状況を把握するために，Web サイトのページ書き換えに関する調査を行なった(図 19).

4.10　1998 年

(1) HIRT セキュリティ情報のサービス開始

1998 年 4 月，CERT/CC，JPCERT/CC や製品ベンダ(シスコ，ヒューレッドパッカード，マイクロソフト，ネットスケープ，サンマイクロシステムズなど)が発行するセキュリティ情報を元に社内メーリングリストと HIRT プロジェクト用の社内 Web サイトにて対策情報の提供を開始した．

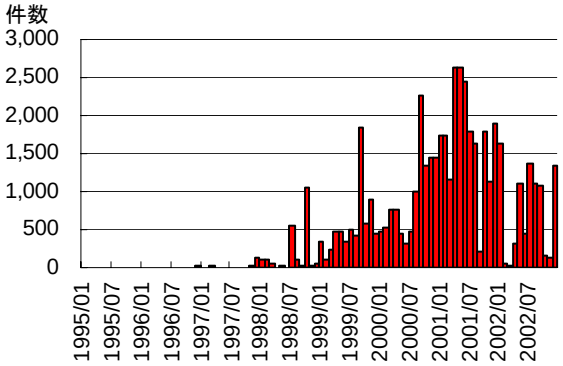


図 19：Web サイトの書き換え件数の推移

(2) ネットワークセキュリティセミナー開催

1998 年 6 月 25 日～26 日，米セキュリティカンファレンス DEFCON[35]にスピーカとしても参加している米国技術者を講師に迎え，日立向けに『ネットワークセキュリティ』教育を実施した．

5　おわりに

冒頭で述べた通り，数年間のインシデントの変遷を見る限り，短いサイクルで新たな侵害活動が生まれ，一度確立した侵害活動は決してなくなることはなく，さらに侵害活動を通して良くも悪くも技術が継承されている．このような状況下において，各組織が保有する観測機能，状況分析機能ならびに対処機能を組織として連携させることによって問題事象の解決を図っていくことが必要であると考えている．

HIRT では，今後共，情報セキュリティ早期警戒パートナーシップを活用した脆弱性対策の推進，複数の CSIRT 同士が協調して新たな脅威に立ち向かうための組織間連携，お互いのインシデント対応活動の改善に寄与できる協力関係の構築を進めていく予定である．

謝辞

日立インシデントレスポンスチーム(HIRT)は，2008 年 10 年 1 日に開催された，情報化月間推進会議(経済産業省，内閣府，総務省，財務省，文部科学省，国土交通省)主催の，平成 20 年度情報化月間記念式典にて，『経済産業省商務情報政策局長表彰(情報セキュリティ促進部門)』を受賞しました[36]．HIRT の活動推進にあたり，ご支援を頂いた社内外関連各位に深く感謝致します．

(2009 年 2 月 19 日)

参考文献

1) NIST NVD (National Vulnerability Database), http://nvd.nist.gov/
2) (独)情報処理推進機構：脆弱性関連情報に関する届出状況, http://www.ipa.go.jp/security/vuln/report/press.html
3) (株)ラック：SQL インジェクション攻撃検知数（2008 年 12 月まで）(2009-01-08), http://www.lac.co.jp/info/alert/alert20090108.html
4) トレンドマイクロ：インターネット脅威レポート, http://jp.trendmicro.com/jp/threat/security_news/monthlyreport/index.html
5) (独)情報処理推進機構：TCP/IP に係る既知の脆弱性検証ツール (2009/1), http://www.ipa.go.jp/security/vuln/vuln_TCPIP_Check.html
6) (独)情報処理推進機構：重要インフラに求められる 高信頼性組織の条件 (2008/2), http://www.ipa.go.jp/security/event/2007/infra-sem/pdf/20080220MEIJI-Nakanishi_sama.pdf
7) (独)情報処理推進機構：DNS キャッシュポイズニング対策 (2009/2), http://www.ipa.go.jp/security/vuln/DNS_security.html
8) Joint Workshop on Security 2008, Tokyo 開催記録サイト (2008/3), http://www.nca.gr.jp/jws2008/index.html
9) NTT-CERT (NTT Computer Security Incident Response and Readiness Coordination Team), http://www.ntt-cert.org/
10) マルウェアの感染方式に基づく分類に関する検討, 情報処理学会 CSEC 研究報告 Vol.2008 No.21. (2008/3)
11) 2008 年ファイル交換ソフトによる情報漏えいに関する調査結果 (2008/12), http://www.hitachi.co.jp/hirt/publications/hirt-pub08008/index.html
12) P2P ファイル交換ソフト環境で流通するマルウェア (2008/12), http://www.hitachi.co.jp/hirt/publications/hirt-pub08007/index.html
13) CSS2008 の CFP を騙ったウイルスメール受信の仮想体験デモ(2009/1), http://www.sdl.hitachi.co.jp/csec/css2008-cfp-malware/malware-demo.html
14) CERT Advisory CA-2002-03, “Multiple Vulnerabilities in Many Implementations of the Simple Network Management Protocol (SNMP)” (2002/2), http://www.cert.org/advisories/CA-2002-03.html
15) CSIRT - 日本シーサート協議会, http://www.nca.gr.jp/
16) WARP (Warning, Advice and Reporting Point), http://www.warp.gov.uk/
17) GlobalSign Adobe Certified Document Services, http://www.globalsign.com/adobe-cds/index.htm
18) FIRST (Forum of Incident Response and Security Teams), http://www.first.org/
19) 経済産業省告示第 235 号：ソフトウエア等脆弱性関連情報取扱基準 (2004/7), http://www.meti.go.jp/policy/netsecurity/downloadfiles/vulhandlingG.pdf
20) (独)情報処理推進機構：情報セキュリティ早期警戒パートナーシップガイドライン (2008/7), http://www.ipa.go.jp/security/ciadr/partnership_guide.html
21) JVN (Japan Vulnerability Notes), http://jvn.jp/
22) NISCC: NISCC Vulnerability Advisory 006489/H323: Vulnerability Issues in Implementations of the H.323 Protocol (2004/1), http://www.kb.cert.org/vuls/id/JSHA-5V6H7S
23) Organization for Internet Safety: Draft Security Vulnerability Reporting and Response Process (2003/7), http://www.oisafety.org/resources.html
24) (独)情報処理推進機構：セキュリティ脆弱性情報等の公開ポリシーに関する資料 (2003/9), http://www.ipa.go.jp/security/awareness/vendor/vulnerability200309012.pdf
25) (株)ラック：脆弱性報告と公開のポリシー (2003/8), http://www.lac.co.jp/info/advisory/pdf/vulnerability_reporting_and_disclosure.pdf
26) CERT/CC Vulnerability Disclosure Policy, http://www.cert.org/kb/vul_disclosure.html
27) US-CERT: Vulnerability Note VU#459371: Multiple IPsec implementations do not adequately validate authentication data” (2002/10), http://www.kb.cert.org/vuls/id/459371
28) JPCERT/CC Vendor Status Notes DB 構築に関する検討, CSS2002 (2002/10), http://jvn.doi.ics.keio.ac.jp/nav/CSS02-P-97.pdf
29) セキュリティ情報流通を支援する JVN の構築 (2005/5), http://www.sdl.hitachi.co.jp/japanese/people/jvn/
30) CERT/CC Vulnerability Notes Database, http://www.kb.cert.org/vuls
31) CERT/CC Vulnerability Note Field Descriptions, http://www.kb.cert.org/vuls/html/fieldhelp
32) CVE (Common Vulnerabilities and Exposures), http://cve.mitre.org/
33) ICAT, http://icat.nist.gov/
34) CVSS (Common Vulnerability Scoring System), http://www.first.org/cvss/
35) DEFCON, http://www.defcon.org/
36) 情報化月間 2008-平成 20 年度情報化促進貢献企業等表彰 (2008/10), http://www.jipdec.or.jp/gekkan/ceremony/prize02.html

執筆者
寺田真敏（てらだ まさと）
1998 年に HIRT の試行活動を立ち上げて以降，2002 年に JVN(http://jvn.jp/)の前身となる研究サイト(http://jvn.doi.ics.keio.ac.jp/)の立ち上げ，2005 年には HIRT の窓口として CSIRT の国際団体である FIRST への加盟など対外的な CSIRT 活動を推進．現在，JPCERT コーディネーションセンター専門委員，(独)情報処理推進機構研究員，日本シーサート協議会の副運営委員長を務める．